PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-204330**
(43)Date of publication of application : **05.08.1997**

(51)Int.Cl. G06F 12/00
G06F 12/00
G06F 3/14
G06F 12/14
G09C 1/00
G09C 1/00
H04L 9/08
H04L 9/32

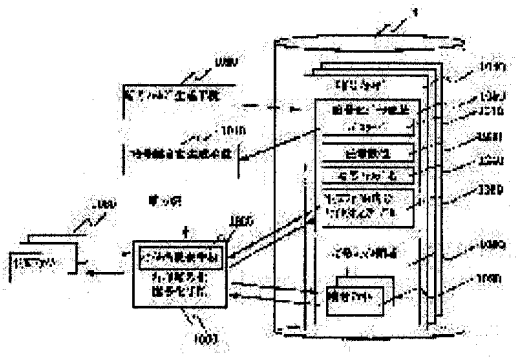
(21)Application number : **08-283854**
(22)Date of filing : **25.10.1996**

(71)Applicant : **HITACHI LTD**
(72)Inventor : **OTE ICHIRO**
IWABUCHI KAZUNORI
WASHIMI HIROAKI
FURUKAWA HIROSHI
SUMITOMO MASATO
KOBAYASHI YUICHI

(30)Priority
Priority number : **07279325** Priority date : **26.10.1995** Priority country : **JP**

(54) DEVICE AND METHOD FOR CIPHERING AND DECIPHERING INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To release a user from the managing of a cipher key and cipher file by generating a cipher folder on a storage device and allowing a ciphering and deciphering means to cipher a selected plain text file so as to automatically store and manage.
SOLUTION: When ciphering is instructed from the user, the file ciphering and deciphering means 1000 automatically generates the cipher key from the password 1070 of a cipher folder 1040 specified by the user by a cipher key automatic generation means 1010. Then through the use of the cipher key, the means 1000 ciphers a specified normal sentence file 1030 to store in a cipher file area 1080 in the cipher folder 1040 as a cipher file 1090. In addition, at the time of this storing, through the use of a file name converting means 1220, each file 1090 is stored by using individually unique internal name so as to make the cipher folder 1040 an area hidden from the user. At the time of deciphering, a corresponding normal sentence file 1030 and the name of the cipher file are stored in a plain text file/cipher file corresponding table 1060 so as to return to the original normal sentence file.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（A）　(11)特許出願公開番号

特開平9－204330

(43)公開日　平成９年(1997)８月５日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/00	５１５		Ｇ０６Ｆ	12/00	５１５Ｍ
		５３７				５３７Ｈ
	3/14	３７０			3/14	３７０Ａ
	12/14	３２０			12/14	３２０Ｂ
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ａ

審査請求　未請求　請求項の数18　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平8－283354

(22)出願日　平成８年(1996)10月25日

(31)優先権主張番号　特願平7－279325

(32)優先日　平７(1995)10月26日

(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　大手　一郎
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　岩渕　一則
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　鷲見　浩明
愛知県名古屋市中区栄三丁目10番22号日立中部ソフトウェア株式会社内

(74)代理人　弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　情報の暗号化、復合化装置および方法

(57)【要約】　（修正有）

【課題】金庫を模倣しアイコンを対象として、ドラッグアンドドロップという直感的な操作により、ファイル暗号化の操作を実現し、さらに、ユーザ認証用のパスワードから自動的にファイルの暗号化・復号化に使う暗号鍵を生成し、暗号鍵に関する操作を一切ユーザから隠蔽するなど、エンドユーザ向けの簡単操作のファイル暗号化制御装置と方法を提供する。

【解決手段】暗号化・復号化を行うユーザ・インターフェイス部１１１と、パスワード１２１１から暗号鍵を自動生成する暗号鍵生成・登録手段１１４と、パスワードによる認証を行なうことなくファイル暗号処理をするファイル暗号化、復号化手段１１６，１１７とを備え、操作性の優れたファイル暗号化機能を提供する。

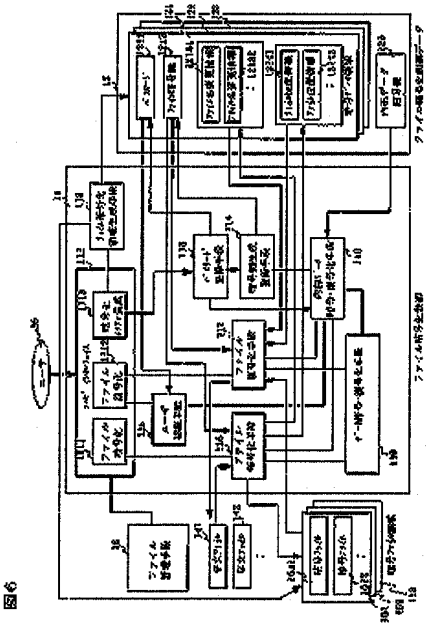


図６

1

【特許請求の範囲】

【請求項１】計算機上の情報の暗号化・復号化を行うデータ暗号化システムにおいて、ユーザが指定した平文ファイルを暗号鍵により暗号化、および、復号化するファイル暗号化復号化手段と、前記ファイル暗号化復号化手段により特定の暗号鍵を使用して暗号化した少なくとも一つの暗号ファイルを格納し、ファイルを管理するための暗号情報を格納する格納領域手段と、前記暗号情報格納領域手段にユーザがアクセスする際の認証パスワードを登録するためのパスワード登録手段を含む情報の暗号化、復合化装置。

【請求項２】前記平文ファイルのファイル名を前記暗号情報格納領域手段の内部的な暗号ファイルのファイル名に変換するファイル名変換手段、前記平文ファイル名と前記暗号ファイル名とのファイル名対応テーブル、および、前記暗号情報格納領域手段に入力された暗号化に関連する内部データを暗号化するための内部データ暗号化復号化手段を含み、それにより前記暗号情報格納領域をユーザから隠蔽する請求項１記載の情報の暗号化、復合化装置。

【請求項３】前記認証パスワードに基づき、前記暗号鍵を自動生成する暗号鍵自動生成手段を含み、前記ファイル暗号化復号化手段は、前記暗号鍵自動生成手段により自動生成した暗号鍵によりファイルの暗号化、および、復号化を行う請求項１記載の情報の暗号化、復合化装置。

【請求項４】前記暗号情報格納領域手段に入力された、暗号化に関連する内部データを暗号化するための内部データ暗号化復号化手段を含み、前記認証パスワードを前記内部データ暗号化復号化手段により暗号化してパスワード登録手段の前記認証パスワード記憶領域に登録保持し、前記平文ファイルの暗号化の際に、前記認証パスワードを復号化し、前記暗号鍵自動生成手段により暗号鍵を自動生成し、前記暗号鍵を使用して、ファイルの暗号化を行う請求項３記載の情報の暗号化、復合化装置。

【請求項５】特定回数以上入力された不正な認証パスワードがに応答して、前記暗号情報格納領域手段を無効化する暗号情報格納領域無効化手段を備える請求項１記載の情報の暗号化、復合化装置。

【請求項６】前記暗号情報格納領域無効化手段により無効にした前記暗号情報格納領域手段を再び前記暗号情報格納領域手段として利用可能とするための暗号情報格納領域バックアップ手段を備える請求項５記載の情報の暗号化、復合化装置。

【請求項７】記憶装置上に、前記暗号情報格納領域手段を複数生成し、前記暗号鍵、および、前記認証パスワードをそれぞれ独立に割り当てるための暗号情報格納領域生成手段を備える請求項１記載の情報の暗号化、復合化装置。

【請求項８】前記暗号情報格納領域手段に格納された前記暗号ファイルの暗号化以前の記憶装置上での位置情報テーブルを前記暗号情報格納領域手段に備え、前記暗号ファイルの復号化の際に、復号化後の平文ファイルを記憶装置上の元の位置に自動的に戻す請求項１記載の情報の暗号化、復合化装置。

【請求項９】前記暗号情報格納領域手段の全てのデータを他の計算機に転送可能な外部ファイルに変換する外部ファイル変換手段、および、前記外部ファイルから前記暗号情報格納領域手段を再生成する暗号情報格納領域生成手段を備え、他の計算機への前記暗号情報格納領域手段の情報の転送を可能とする請求項１記載の情報の暗号化、復合化装置。

【請求項１０】他の計算機に転送して実行し、前記認証パスワードの入力により、前記暗号情報格納領域手段内の前記暗号ファイルを自動的に復号化可能な自己復号化プログラム・ファイルを前記暗号情報格納領域手段の全てのデータをファイル復号化処理プログラムに統合して生成する自己復号化プログラム生成手段を備える請求項１記載の情報の暗号化、復合化装置。

【請求項１１】ファイル暗号化の操作対象として計算機のディスプレイの画面上に金庫のような暗号装置を容易にイメージさせるグラフィック・メタファを表示し、ファイルの選択操作と前記グラフィック・メタファの選択操作という単純な連続操作に応答してファイルの暗号化を行うユーザ・インターフェイス手段を備える請求項１記載の情報の暗号化、復合化装置。

【請求項１２】計算機上の情報の暗号化及び復号化を装置を用いて行う情報の暗号化、復合化方法は以下のステップを含む：前記情報としての平文ファイルを暗号化した暗号化ファイルを記憶する暗号化ファイル領域と、平文ファイル名と暗号化ファイル名とを対応させて記憶する暗号化データ領域と、ユーザが入力したパスワードをシステム鍵によって暗号化したパスワードを記憶するパスワード記憶領域とを特定した記憶エリア（記憶フォルダ）を設けること；暗号化において、

暗号化ユーザが入力したパスワードをシステム鍵を用いて暗号化パスワードを生成し、前記パスワード記憶領域に記憶すること；暗号化パスワードをシステム鍵によって復号化し、暗号鍵を生成すること；前記暗号鍵を用いて、指定された平文ファイルを暗号化して、暗号化平文ファイルを前記暗号化ファイル領域に格納すること；および平文ファイル名と暗号化ファイル名の対応を表わすテーブルを前記暗号化データ領域に登録すること；復号化において、

復号化ユーザが入力したパスワードに基づき、暗号化データ領域の前記登録対応テーブルを表示すること；前記表示テーブルを参照して、復号化すべきファイル名をユーザーにより指定すること；前記入力パスワードに基づき、前記復号鍵を生成すること；前記生成した復号鍵を用いて、前記指定されたファイル名の暗号化ファイルを

復号化すること。

【請求項１３】請求項１２情報の暗号化、復合化方法において、前記復号化において、復号化ユーザーのパスワードの入力に応答して、その入力したパスワードを、前記パスワード記憶領域に記憶されたパスワード照合し、認証の結果に応じて、復号化プロセスの実行を許否する。

【請求項１４】請求項１２情報の暗号化、復合化方法において、前記記憶エリアを複数設定し、各エリアを区別化して表わすメタファアイコンにより、表示画面上に表示することを含む。

【請求項１５】請求項１４情報の暗号化、復合化方法において、前記表示画面上に表示されたファイル名をポインティング装置により指定し、かつ重畳関係で該装置で前記複数記憶エリアを表示するアイコンの１つを特定することにより、復号化操作（プロセス）を起動することを含む。

【請求項１６】請求項１２情報の暗号化、復合化方法において、前記復号化において、前記ファイル名は記憶エリア内の暗号ファイル領域に格納された暗号化されたファイルを表わす。

【請求項１７】計算機上で、情報の暗号化及び復号化の動作を指示するための計算機で読み取り可能なメモリ媒体は以下を含む：前記情報としての平文ファイルを暗号化した暗号化ファイルを記憶する暗号化ファイル領域と、平文ファイル名と暗号化ファイル名とを対応させて記憶する暗号化データ領域と、平文ファイル名と暗号化ファイル名とを対応させて記憶する暗号化データ領域と、ユーザが入力したパスワードをシステム鍵によって暗号化したパスワードを記憶するパスワード記憶領域とを特定した記憶エリア（記憶フォルダ）を設ける手段；暗号化において、

暗号化ユーザが入力したパスワードをシステム鍵を用いて暗号化パスワードを生成し、前記パスワード記憶領域に記憶する手段；暗号化パスワードをシステム鍵によって復号化し、暗号鍵を生成する手段；前記暗号鍵を用いて、指定された平文ファイルを暗号化して、暗号化平文ファイルを前記暗号化ファイル領域に格納する手段；および平文ファイル名と暗号化ファイル名の対応を表わすテーブルを前記暗号化データ領域に登録する手段；復号化において、

復号化ユーザが入力したパスワードに基づき、暗号化データ領域の前記登録対応テーブルを表示する手段；前記表示テーブルを参照して、復号化すべきファイル名をユーザにより指定する手段；前記入力パスワードに基づき、前記復号鍵を生成する手段；前記生成した復号鍵を用いて、前記指定されたファイル名の暗号化ファイルを復号化する手段。

【請求項１８】請求項１７の媒体において、前記復号化において、復号化ユーザのパスワードの入力に応答して、その入力したパスワードを、前記パスワード記憶領域に記憶されたパスワードと照合し、認証の結果に応じて、復号化プロセスの実行を許否する手段を含む。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、個人情報や秘密情報を暗号化して保持し、第三者への情報漏洩を防止する情報システムと方法に関する。

【０００２】

【従来の技術】ノート型パーソナル・コンピュータ（以後、PCと称す）やペン入力PC等、高性能、かつ、携帯性の高い計算機の普及により、出張先等、事務所外でのさまざまな場所で、計算機を業務を目的として利用する機会が増加してきている。こうした携帯型の計算機の普及に伴って、計算機の盗難、紛失による情報漏洩が問題となりつつある。

【０００３】一方，マルチメディア化等に伴って家庭でもPCを始めとする計算機が普及してきている。このような家庭向けの計算機では、家族で共有して計算機を使うことが多く、個人情報の保護機能が必要となりつつある。

【０００４】こうした計算機の携帯化や家庭への浸透等により、業務に関連した機密情報や個人情報の漏洩に対するエンドユーザ・レベルでのセキュリティ機能に対してのニーズが高まりつつある。

【０００５】これらのニーズに対応したセキュリティ機能としては、機密情報ファイルや個人情報ファイルを暗号鍵を用いて暗号化して、暗号鍵を所持しない第三者からの情報アクセスから保護するファイルの暗号化機能が、有効な手法として知られている。

【０００６】

【発明が解決しようとする課題】ところで、従来のファイル暗号化機能では、第三者に秘密とする暗号鍵を暗号処理に用いるため、ファイル暗号化や復号化の際に、パスワードの入力による暗号鍵のオープン操作等の準備操作が必要であったり、暗号鍵の管理をユーザが行う必要があった。また、暗号化したファイルの管理についてもユーザに任されており、例えば、ファイルを後で復号化するためにどの暗号鍵で暗号化したファイルかをユーザ責任で記憶しておく必要があった。このように従来のファイル暗号化機能は、専門知識を必要としたり、操作が繁雑でエンドユーザには操作が難しく、気軽に利用できないという問題があった。したがって、ファイル暗号化等の高度なセキュリティ機能は、一般に、一部の専門的な業務を行うユーザ向けのものとなっていた。

【０００７】本発明者は、暗号鍵を自動生成することによりユーザが暗号鍵を意識することなくファイルの暗号化復号化を行えること、また、特定の暗号鍵により暗号化した暗号ファイルを一括管理することによりユーザの一つ一つの暗号ファイルの管理が不要になること、さら

に．ファイルの復号化の操作の際にのみユーザの認証を行えば必ずしも暗号化の操作の際にユーザの認証を行わなくても暗号化したファイルの保護を行えることに着目した。

【０００８】従って、本発明は、上記着目点に基づき、暗号鍵と暗号ファイルの管理からユーザを解放し．また．画面上で平文ファイルを選択しアイコン等のグラフィック・メタファにより暗号化処理を起動するという単純な操作で、ファイルの暗号化を可能とする情報の暗・復号化装置と方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記目的を達成するために．本発明の一つの態様による情報の暗・復号化装置は．ユーザが指定した平文ファイルを暗号鍵により暗号化．および、復号化する暗号化復号化手段と、特定の暗号鍵を使用して前記暗号化復号化手段により暗号化した暗号ファイルを一括して格納・管理する記憶装置上の暗号情報格納手段（以後、暗号フォルダと呼ぶ）と．記憶装置上に前記暗号フォルダを複数生成し、前記暗号鍵、および、前記認証パスワードをそれぞれ独立に割り当てる暗号フォルダ生成手段と．前記暗号フォルダにユーザがアクセスする際の認証を行うための認証パスワードを格納する格納手段を含む。

【００１０】さらに、本発明の別の態様によれば．前記暗号化制御装置は、前記暗号フォルダ内部の暗号化に関連する内部データを暗号化するための内部データ暗号化復号化手段と．前記記平文ファイルのファイル名を前記暗号フォルダの内部的な暗号ファイル名に変換するファイル名変換手段と、前記暗号フォルダ内部に前記平文ファイル名と変換した前記暗号ファイル名との対応テーブルを含む。

【００１１】本発明の別の態様によれば、前記暗号化制御装置は、前記認証パスワードを基に暗号鍵を自動生成する暗号鍵自動生成手段と．前記暗号フォルダ内部に、認証パスワードを登録保持するための認証パスワード記憶領域を含む。

【００１２】本発明による暗号化制御装置の動作の概要を説明すると．あらかじめ．前記暗号フォルダ生成手段により記憶装置上に暗号フォルダを生成しておくことで．ユーザが選択した平文ファイルは．前記暗号化復号化手段が前記暗号フォルダに割り当てられた前記暗号鍵を使用して暗号化し、自動的に前記暗号フォルダ内に格納して、一括して記憶・管理するために、ユーザによる暗号ファイル毎の個別な管理を不要とすることができる。また、前記暗号化復号化手段は．ユーザが暗号フォルダにアクセスしてファイルの暗号化・復号化を行う際に．それぞれ前記暗号フォルダに割り当てられた前記認証パスワードにより、正しいユーザか否か認証を行い、前記暗号フォルダに対する不正アクセスから保護する。

【００１３】前記暗号フォルダ内に格納された前記暗号ファイル名は．前記ファイル名変換手段により．ユーザが認識している前記平文ファイルから内部的な暗号ファイルに変換し．また、前記暗号フォルダ内部の暗号ファイルを記憶・管理するための内部データについても、前記内部データ暗号化復号化手段により暗号化することで．前記暗号フォルダに格納された前記暗号ファイルをユーザから隠蔽し、内部データに対するユーザの不正なアクセスや誤操作から保護可能となる。

【００１４】前記暗号鍵自動生成手段は、前記暗号フォルダにアクセスするためにユーザが入力した前記認証パスワードを基に前記暗号鍵を自動生成し、煩雑なユーザによる前記暗号鍵の操作・管理を不要とする。

【００１５】さらに、暗号化フォルダ生成時に．前記暗号フォルダ生成手段が前記暗号フォルダ内部に前記認証パスワード記憶領域を設定し、ユーザが入力した前記認証パスワードを前記内部データ暗号化復号化手段により暗号化して前記認証パスワード記憶領域に登録・保持した場合には、前記暗号化復号化手段は．前記認証パスワード入力による認証を省略して、前記前記認証パスワード記憶領域に登録した前記認証パスワードを読み出し、前記内部データ暗号化復号化手段により復号化して、前記暗号鍵自動生成手段により暗号鍵を自動生成してファイルの暗号化を行う。したがって、ユーザは、前記認証パスワードの入力を行うこともなく平文ファイルを選択して前記暗号化復号化手段を起動するといった非常に単純な操作でファイルの暗号化を行うことが可能となる。

【００１６】特に、前記暗号フォルダ生成手段が．前記暗号フォルダ生成時に、金庫等の暗号装置をユーザにイメージさせるアイコン等のグラフィック・メタファを前記暗号フォルダ毎に計算機の画面上に表示し、さらに、前記グラフィック・メタファの選択操作を契機に前記暗号化復号化手段が起動するようにしておくと、マウス等のポインティングデバイスにより画面上でファイル管理機能から平文ファイルを選択し、そのまま、前記グラフィック・メタファを選択するという画面上での単純で直感的な操作によりファイルの暗号化が可能となり．一般ユーザ向けの操作性の良い暗号化機能を提供できる。

【００１７】

【発明の実施の形態】以下．本発明の実施例を図面を参照して説明する。図２は．本発明の暗号化制御装置を実現するシステムの基本構成を示す。１はCPU．２はROM．３はRAM．４はディスク装置、５はディスプレイ装置．６はキーボード．７はマウス、８はシステム・バスを表わす。本発明を実現する各制御プログラムはあらかじめディスク４上に格納し、RAM4上にロードし．CPU1により制御実行する。また、各データ領域は、RAM4上で処理した後に、保存の必要なデータは．ディスク４上に格納する。

【００１８】図１は、本発明を実現する一実施例のブロック図を示し．本発明の基本構成について説明する。１

０００は、暗号鍵を用いて、ファイルの暗号化と復号化を行うファイル暗号化復号化手段、１２２０は、平文ファイル名から内部的な暗号ファイル名にファイル名を変換するファイル名変換手段、１０１０は、本発明の特徴となるパスワードからの暗号鍵の自動生成を行う暗号鍵自動生成手段を表わし、１０３０は、暗号化の対象となる平文ファイル、１０４０は、ディスク４上の本発明の特徴となる暗号フォルダを表わし、暗号フォルダは平文１０３０を暗号化した暗号ファイル１０９０を格納する暗号ファイル領域１０８０と前記暗号フォルダ１０４０を管理するための情報を格納する暗号化データ領域１０５０から構成する。また、暗号化データ領域１０５０は、暗号化する前の平文ファイル名と暗号化後の暗号ファイル名の対応を管理するための平文ファイル／暗号ファイル対応テーブル１０６０、ユーザが暗号フォルダにアクセスするための認証に使うパスワード１０７０、暗号鍵自動生成手段１０１０が、パスワード１０７０から暗号鍵を自動生成する際に使用する任意数値１２３０、暗号フォルダ名１２４０を格納し、それぞれの格納領域を含む。１０２０は、暗号フォルダ１０４０を生成する暗号フォルダ生成手段を表わし、ディスク４上に複数の暗号フォルダの生成を可能とする。

【００１９】本実施例では、ファイルの暗号化を行うために、初期設定として暗号フォルダ生成手段１０２０により、ディスク４上に、一つ以上の暗号フォルダ１０４０を生成する。暗号化フォルダ生成手段１０２０は、ディスク４上に、暗号フォルダ１０４０を構成するディレクトリを生成し、そのディレクトリ内に、暗号化データ領域１０５０を構成するファイルと暗号ファイル領域１０８０を構成するサブディレクトリを作成する。さらに、暗号フォルダ１０４０作成時には、ユーザに対して、パスワード１０７０、任意数値１２３０、暗号フォルダ名１２４０の入力を要求し、ユーザが入力したパスワード１０７０、任意数値１２３０、暗号フォルダ名１２４０を暗号化して、暗号化データ領域１０５０に格納する。暗号化データ領域１０５０に格納するデータの暗号化は、参照できないようにするため、これら内部データの暗号化専用に用意した暗号鍵により行う。

【００２０】ファイル暗号化復号化手段１０００が暗号化を行うための暗号鍵は、暗号化あるいは復号化を行う際に、暗号鍵自動生成手段１０１０が、暗号化データ領域１０５０に暗号化して格納したパスワード１０７０と任意数値１２３０から生成する。暗号鍵自動生成手段１０１０は、パスワード１０７０と任意数値１２３０を取り出し、復号化して、これらに適当なビットシフト等のビット操作や演算を施しながら合成し、暗号フォルダ毎にユニークな暗号鍵を自動的に生成する。任意数値１２３０は、パスワード１０７０から暗号鍵を生成するために十分なビットサイズを持った数値とし、暗号フォルダ１０４０生成時に一度だけユーザから入力する。また、

暗号鍵は、後述する実施例のように、暗号フォルダ生成時に、暗号鍵自動生成手段１０１０が、登録されたパスワード１０７０から自動生成し、パスワードと共に暗号化データ領域１０５０に暗号化して格納する方法もある。この場合、暗号化の際に、登録した暗号鍵を利用できるので、逐次、暗号鍵を生成する必要はない。

【００２１】平文ファイル１０３０の暗号化は、ファイル暗号化復号化手段１０００によって行う。ユーザからのファイル暗号化の指示があるとファイル暗号化復号化手段１０００は、まず、暗号鍵自動生成手段１０１０によりユーザが指定した暗号フォルダ１０４０のパスワード１０７０から暗号鍵を自動生成する。そして暗黙に自動生成した暗号鍵を使用して、ユーザが指定した平文ファイル１０３０を暗号化して暗号フォルダ１０４０の暗号ファイル領域１０８０に暗号ファイル１０９０として格納する。このように、暗号フォルダ生成時に、あらかじめ、暗号フォルダ１０４０内にパスワード１０７０を格納しておき、それを基に暗号鍵を自動生成し、その暗号鍵によりファイルの暗号化を行うことにより、ユーザがパスワード入力による認証や暗号鍵のオープン処理等することなく、ファイル選択とファイル暗号化復号化手段１０００の起動という単純な操作だけでファイルの暗号化が可能となる。

【００２２】また、ファイル暗号化復号化手段１０００は、暗号ファイル１０９０を格納する際、ファイル名変換手段１２２０により暗号ファイル１０９０ごとにそれぞれユニークな内部名を生成し、その名前を使って、暗号ファイル１０９０を暗号ファイル領域１０８０に格納して、暗号フォルダ１０４０をユーザから隠蔽された領域とする。復号化の際に、元の平文ファイルに戻すために、対応する平文ファイル１０３０の名前と暗号ファイル１０９０の名前を暗号化データ領域１０５０の平文ファイル／暗号ファイル対応テーブル１０６０に格納する。このように、内部データ暗号化用の暗号鍵による暗号化データ領域１０５０の暗号化、および、ファイル名変換手段１２２０と平文ファイル／暗号ファイル対応テーブル１０６０による暗号ファイル名の変換で、暗号フォルダ１０４０をユーザから隠蔽し、暗号ファイルや暗号鍵の管理からユーザを解放する。

【００２３】平文ファイル１０３０の復号化も、ファイル暗号化復号化手段１０００によって行う。

【００２４】復号化するために、ファイル暗号化復号化手段１０００を起動すると、ファイル暗号化復号化手段１０００は、ユーザ入力パスワードに対するパスワード１０７０による認証処理を行った後、平文ファイル／暗号ファイル対応テーブル１０６０を参照して、暗号ファイル領域１０８０内の暗号ファイル１０９０を平文ファイル名で一覧表示する。この状態は、暗号フォルダ１０４０をオープンした状態で、ユーザは、平文ファイル名での一覧表示の中から暗号ファイル領域１０８０内の暗

号ファイル１０９０を選択し、復号化できる。ユーザが、一覧から暗号ファイル１０９０を一つ以上選択して、再び、ファイル暗号化復号化手段１０００を起動すると、ファイル暗号化復号化手段１０００は、まず、暗号鍵自動生成手段１０１０によりパスワード１０７０から暗号鍵を自動生成する。次に平文ファイル／暗号ファイル対応テーブル１０６０を参照して、ファイル名変換手段１２２０によりユーザが選択した平文ファイル名を暗号ファイル１０９０の名前に変換して、暗号ファイル領域１０８０から取り出す。さらに、自動生成しておいた暗号鍵を使用して復号化し、元の平文ファイル名の平文ファイルに戻す。

【００２５】このように、ファイルの復号化の際にも暗号鍵自動生成手段１０１０やファイル名変換手段１２２０と平文ファイル／暗号ファイル対応テーブル１０６０により、暗号鍵を意識することなく、パスワード１０７０の入力、平文ファイル名による暗号ファイルの選択、そして、ファイル暗号化復号化手段１０００の起動という単純な操作だけでファイルの復号化が可能なる。

【００２６】次に、FD（Floppy Disk）等の媒体やネットワークを通して暗号フォルダを他の計算機への転送することを目的として、暗号フォルダの外部ファイルへの変換を行う実施例について図３により説明する。図３の暗号化フォルダ１０４０は、図１の暗号化フォルダと同一のものである。ユーザから暗号フォルダの外部ファイルへの変換を要求されると、暗号フォルダ・ファイル生成手段１１００は、ユーザが選択した暗号フォルダ１０４０に対応する暗号化データ領域１０５０、暗号ファイル領域１０８０のディレクトリの暗号ファイル１０９０のデータをそれぞれ読み出し、１ファイルに結合して、暗号フォルダ・ファイル１１２０を作成する。暗号フォルダ・ファイル１１２０は、外部ファイルとしてディスク４上の特定のディレクトリやFD１３００に出力する。

【００２７】暗号フォルダ・ファイル１１２０は、FD１３００やネットワーク１４００等を介して、本発明の概念に従うファイル暗号化機能をあらかじめ設定した計算機に転送し、暗号フォルダ生成手段１１１０により再び暗号フォルダ１０４０に復帰できる。暗号フォルダ生成手段１１１０は、暗号フォルダ・ファイル１１２０から暗号化データ領域１０５０と暗号ファイル領域データ１１３０のデータをそれぞれ読み出して、このデータを基に、暗号フォルダ生成手段１０２０と同様にして、転送先の計算機に接続されたディスク４上に暗号化フォルダ１０４０を生成する。この暗号フォルダに格納された暗号ファイルは、図１の実施例とまったく同様に、パスワードを入力することで復号化することが可能となる。

【００２８】図３の実施例では、暗号フォルダ・ファイル１１２０として１ファイルとしたが、計算機のオペレーティングシステム（OS）がディレクトリ毎の転送を支援するような場合は、暗号フォルダのディレクトリ内の

ファイルやディレクトリを適当なディレクトリにまとめて外部ファイル群としてFD１３００等の媒体に格納することももちろん可能である。

【００２９】また、図３の実施例のように、暗号フォルダ・ファイル１１２０を１ファイルで構成した場合、内部に複数暗号ファイルのデータを含むことから暗号フォルダ・ファイル１１２０のサイズが大きくなる場合がある。この場合、暗号フォルダ・ファイル生成手段１１００により暗号フォルダ・ファイル１１２０を生成する際に、データ圧縮処理を行い、再び、暗号フォルダ生成手段１１１０により暗号フォルダ１０４０を生成する際に、伸長処理を行う等により、暗号フォルダ・ファイル１１２０のサイズの縮小化を図ることが可能である。

【００３０】ところで、図３の実施例では、暗号フォルダ・ファイル１１２０を転送する計算機に、本発明の概念に従うファイル暗号化システムをあらかじめ設定されていることが前提となっていた。これは任意の計算機に暗号ファイルを配布するような場合に不便である。そこで、図４の他の実施例では、本発明概念のファイル暗号化システムがあらかじめ設定されていない計算機上でも暗号フォルダ・ファイル内の暗号ファイルを展開できるようにする。

【００３１】自己復号化ファイル生成手段１１４０は、暗号フォルダ１０４０の暗号化データ領域１０５０、暗号ファイル１０９０のデータをそれぞれ読み出し、結合する。さらに、これを復号化対象のデータとして、ファイル暗号化復号化手段１０００の復号化処理と等価な機能を持つ復号化手段１１７０と暗号鍵自動生成手段１０１０とで構成する復号化プログラム１１５０のファイルに連結して、自己復号化プログラム１１６０のファイルを生成する。自己復号化プログラム１１６０は、外部ファイルとしてディスク４上の特定のディレクトリやFD１３００に出力する。

【００３２】自己復号化プログラム１１６０を他の計算機に転送して実行すると、復号化手段１１７０が起動される。復号化手段１１７０は、内部データとして結合された暗号フォルダ１０４０のデータから暗号化データ領域１０５０と暗号ファイル領域データ１１３０のデータをそれぞれ読み出す。そしてユーザにパスワード入力を要求し、パスワード１０７０と照合し、正しいパスワードなら、復号化の処理を開始する。パスワード１０７０から暗号鍵を自動生成して、暗号ファイル１０９０のデータを復号化していく処理は、図１の実施例と同様である。転送先の計算機に接続されたディスク４上の、例えばユーザが指定したディレクトリに、復号化した平文ファイル１０３０を出力して、必要なら、最後に、自己復号化プログラム１１６０自体をディスクから削除し、自己復号化処理を終了する。本実施例により、プログラム実行の可能な任意の計算機のユーザにネットワーク１４００を介して暗号ファイルを暗号フォルダ単位で転送可

能となり、本発明の応用範囲が非常に広がる。

【００３３】次に、暗号フォルダへの不正なアクセスを防止をするための不正パスワード入力回数の限定方法について図５を用いて説明する。図５のファイル暗号化復号化手段１０００、鍵自動生成手段１０１０、暗号フォルダ生成手段１０２０、暗号フォルダ１０４０は、図１と同一構成である。１１８０は、暗号フォルダ１０４０へユーザがアクセスする際に、パスワードで、ユーザ認証を行うための認証手段．１１９０は、認証手段１１８０が、不正なパスワードの入力回数をカウントするためのカウンタ、１２００は、ユーザから不正なパスワードが入力された場合に、暗号化フォルダ１０４０を無効にして暗号フォルダ１０４０への不正なアクセスを防止をするための暗号フォルダ無効化手段．１２１０は、暗号フォルダ無効化手段１２００により無効にした暗号フォルダ１０４０を復帰するために、無効化される前に、暗号化フォルダをバックアップしておくための暗号フォルダ・バックアップ手段を表わす。

【００３４】ファイル暗号化復号化手段１０００は、暗号フォルダ１０４０内の暗号ファイル１０９０の復号化等を行う際、認証手段１１８０により、暗号フォルダ１０４０にアクセスするためのパスワード入力をユーザに要求する。ユーザからパスワードが入力されると、認証手段１１８０は、暗号フォルダ内のパスワード１０７０と比較して、一致した場合、正当なユーザと判断し、ファイル暗号化復号化手段１０００に通知し、ファイル暗号化復号化手段１０００の処理を進める。一方、不正なパスワードが入力されると、認証手段１１８０は、カウンタ１１９０をカウントアップしていく。但し、カウンタ１１９０は、正しいパスワードが入力された時点で、クリアする。不正なパスワードが連続して入力され、カウンタ１１９０の値があらかじめ設定された特定回数、例えば、3回を越えると認証手段１１８０は、暗号フォルダ無効化手段１２００に、暗号フォルダ１０４０を無効とするように指示する。

【００３５】暗号フォルダ無効化手段１２００は、認証手段１１８０から指示を受けると、暗号フォルダ１０４０内のパスワード１０７０を消去する。認証手段１１８０は、パスワード１０７０が消去されていること確認すると認証処理を中止して、ユーザに、暗号フォルダが無効であることをメッセージとして知らせる。したがって、一旦、パスワード１０７０が消去されると、以後、暗号フォルダ１０４０へのアクセスは不可能となる。

【００３６】無効化されると正当なユーザでも暗号フォルダ１０４０へアクセスできなくなるため、正当なユーザが無効となった暗号フォルダ１０４０を復帰させる手段が必要となる。そこで、暗号フォルダバックアップ手段１２１０は、暗号化フォルダ１０４０をバックアップする機能を提供する。

【００３７】暗号フォルダバックアップ手段１２１０

は、暗号フォルダ１０４０のバックアップの際に、パスワード１０７０の内容を、例えば、FD１３００のようなリムーバブルな媒体にコピーする。さらに、暗号フォルダ名１２４０を暗号フォルダ１０４０を特定する情報としてFD１３００に記録する。復帰の際には、暗号フォルダ名１２４０を比較して、バックアップされているFD１３００の内容と暗号フォルダ１０４０が一致していることを確認し、FD１３００にバックアップされたパスワード１０７０を暗号フォルダ１０４０にコピーし、暗号フォルダ１０４０を元の状態に戻す。

【００３８】バックアップに使用したFD１３００が不正な復帰処理に使われることを防止するには、FD１３００による復帰の際に、暗号フォルダ名１２４０を比較した後、ユーザにパスワード入力を要求し、FD１３００内のパスワード１０７０との一致をチェックすることにより、第三者による不正な復帰処理を防止できる。

【００３９】この暗号フォルダバックアップ手段１２１０により、ユーザは、暗号化フォルダ１０４０が無効化に備え、事前に暗号フォルダのバックアップをFD１３００等に取って置くことで、暗号フォルダ１０４０が不正なパスワード入力により無効化された場合でも、FD１３００を使って暗号フォルダ１０４０を復帰し、再び、アクセスすることが可能となる。

【００４０】また、暗号フォルダバックアップ手段１２１０のバックアップ操作は、パスワードによる認証後に可能とし、復帰操作は、随時行えるようにすることで、正当なユーザのみが暗号フォルダ１０４０をバックアップし、無効化された状態でも復帰可能となり、第三者による不正なバックアップを防止することができる。

【００４１】図６に、本発明の一実施例のブロック図を示し、さらに詳細に説明する。

【００４２】１１は、本発明を実現するファイル暗号化制御プログラムである。１１１は、ユーザがファイル暗号化を行うためのユーザ・インターフェイス部である。１１１１は、ファイル暗号化のユーザ・インターフェイスである。このユーザ・インターフェイス１１１１は、本発明特徴となる簡便なファイル暗号化の操作を実現する。１１１２は、ファイル復号化のユーザ・インターフェイスである。１１１３は、ユーザがファイル暗号化を行うための操作対象となるメタファを登録するファイル暗号化メタファ登録のユーザ・インターフェイスである。この暗号化のメタファを用いて、ユーザ・インターフェイス１１１１は、前述の簡便なファイル暗号化の操作を実現する。１１２は、ファイル暗号化に必要なデータ領域をディスク４上に確保するファイル暗号化領域生成手段である。１１３は、ユーザの認証に必要となるパスワードをあらかじめ登録するパスワード登録手段である。１１４は、ファイルの暗号化に必要な暗号鍵を生成し、登録する暗号鍵生成・登録手段である。この暗号鍵生成・登録手段は、ユーザが入力したパスワードを用い

て．本実施例の特徴である暗号鍵の自動生成を行う。１１５は、ユーザが入力したパスワードとあらかじめ登録したパスワードを比較してユーザの認証を行うユーザ認証手段である。１１６は．ファイル単位で暗号化を行うファイルの暗号化手段である。１１７は、ファイル単位で復号化を行うファイル復号化手段である。１１８は、暗号化したファイルの機密性を保持するために内部データの暗号化を実現する内部データ暗号・復号化手段である。１１９は．与えられた暗号鍵を用いてデータを暗号・復号化するデータ暗号・復号化手段である。

【００４３】１２は、ファイル暗号化制御プログラム１１を制御するためのファイル暗号化制御データである。このファイル暗号化制御データは、メモリ上で処理し、システム再スタート時にも有効とするためディスク４上に保存する。１２１、１２２、１２３は、ファイル暗号化制御データ１２の内、暗号化したファイルの機密性を保持するために．暗号化してディスク４に格納する必要のある制御データを格納する暗号データ領域である。１２１１は、ユーザが入力したパスワードのデータ．１２１２は、自動生成したファイル暗号鍵のデータ．１２１３１．１２１３２は、暗号化したファイルをユーザから隠蔽するために名前を変更した際の元の平文ファイル名と変更後の暗号ファイル名の対応関係を保持したファイル名変更情報．１２１４１．１２１４２は、暗号化した平文ファイルが暗号化する前に存在したディスク４上でのファイル位置情報である。１２０は．内部データを暗号化するための内部データ暗号鍵である。

【００４４】１３は、ユーザがディスク装置４上のファイルを操作・管理するための管理機能を提供するファイル管理手段である。

【００４５】１４１、１４２は、ディスク４上に格納され．暗号化の対象となる平文ファイルである。本実施例では．暗号化する平文ファイル１４１．１４２等をユーザの指示に従って、ファイル暗号化制御プログラム１１に対して、通知するためにファイル管理手段を利用する。

【００４６】１５１、１５２、１５３は、暗号化したファイルのデータ１５１１．１５１２等を格納するために．ディスク４上に確保した暗号ファイル領域である。

【００４７】図６の構成要素と図１の構成要素の対応関係は．ファイル暗号化領域生成手段１１２、パスワード登録手段１１３は、暗号フォルダ生成手段１０２０に、暗号鍵生成・登録手段１１４は．暗号鍵自動生成手段１０１０に、ファイル暗号化手段１１６．ファイル復号化手段１１７、データ暗号・復号化手段１１９は．ファイル暗号化・復号化手段１０００に、暗号データ領域１２１．１２２、１２３は、暗号化データ領域１０５０に、パワード１２１１は、パスワード１０７０に、ファイル名変更情報１２１３１、１２１３２は．平文ファイル／暗号ファイル対応テーブル１０６０に．平文ファイル１４１．１４２は．平文ファイル１０３０に、暗号ファイル領域１５１．１５２、１５３は、暗号ファイル領域１０８０に、暗号１５１１．１５１２は．暗号ファイル１０９０に、それぞれ対応する。

【００４８】次にファイル暗号化メタファ登録の手順、ファイル暗号化の手順、ファイル復号化の手順についてフローチャートを用いて説明する。

【００４９】図７は、ファイル暗号化メタファ登録時の処理手順をフローチャートで示す。ユーザがユーザ・インターフェイスである暗号化メタファ生成手段（プログラム）１１１３を操作してファイル暗号化メタファ登録処理を起動すると（ステップ５００１）、ユーザ・インターフェイス１１１３は．まず、ファイル暗号化領域生成手段１１２を制御して．暗号データ領域１２１をディスク４上のファイルとして．暗号ファイル領域１５１をディスク４上のディレクトリとして作成する（ステップ５００２）。これらのファイル、および、ディレクトリは．例えば、暗号化制御プログラム１１を格納したディスク４上のディレクトリ下に作成する。また、本実施例では．ユーザがユーザ・インターフェイス１１１３により暗号化のためのメタファを複数生成することを可能とするため、ユーザが、メタファの生成を行う毎に．ファイル暗号化領域生成手段１１２によって、暗号化データ領域１２２、１２３等を．また、暗号ファイル領域１５２．１５３等を随時生成していく。これにより．ユーザは．それぞれ独立したメタファを操作して、独立に設定したおいた暗号化ファイルの格納領域にファイル分類して格納することが可能となる。ユーザは、例えば．ユーザ毎またはファイル種類毎に、ファイルを分類して暗号化し．保存することが可能となる。次に、ユーザ・インターフェイス１１１３は．ユーザにパスワード入力を要求する（ステップ５００３）。ユーザが入力したパスワードは、パスワード登録手段１１３に渡す。パスワード登録手段１１３は、ユーザが入力したパスワードを内部データ暗号鍵１２０を用いて、内部データ暗号・復号化手段１１８により暗号化する。内部データ暗号・復号化手段１１８は．データ暗号・復号化手段１１９によりデータの暗号化を行う。パスワードを暗号化するとパスワード登録手段１１３は、パスワード１２１１としてディスク４に格納する（ステップ５００４）。パスワード登録手段１１３は．パスワードの登録が終わると．暗号化する前のパスワードを暗号鍵生成・登録手段１１４に渡す。パスワードが渡されると暗号鍵生成・登録手段１１４は．例えば．パスワードとあらかじめ各暗号データ領域に対してユニークになるように割り当てられた数値とを合成し、ビット操作等を行うことにより、暗号鍵を自動的に生成する。さらに．暗号鍵生成・登録手段１１４は．生成した暗号鍵を内部データ暗号鍵１２０．および．内部データ暗号・復号化手段１１８により暗号化して．ファイル暗号鍵１２１２としてディスク４に格納す

る（ステップ５００５）。以上のような暗号ファイル領域１５１、１５２、１５３、および、暗号データ領域１２１、１２２、１２３の生成・登録処理を終了すると、最後に、ファイル暗号化を行うためのメタファの登録処理を行う（ステップ５００６）。このメタファの登録に関しては、後述の実施例で説明する。

【００５０】次に、図８のフローチャートにより、ファイル暗号化時の処理手順について説明する。前述の暗号化メタファの登録処理を行った後、ユーザが、ファイル暗号化制御プログラム１１を実行すると（ステップ６００１）、ユーザ・インターフェイス１１１１は、まず、ユーザがファイル暗号化処理の操作を行うためのファイル暗号化のメタファを表示する。ユーザが、マウス７のようなポインティング・デバイスを操作して、ファイル管理手段１３のユーザ・インターフェイス上で暗号化する平文ファイルを選択し、さらに、続けて、ファイル暗号化メタファを選択すると、ユーザ・インターフェイス１１１１は、選択された平文ファイルを対象として、ファイル暗号化処理を開始する（ステップ６００２）。これらのユーザ・インターフェイスについては、後述の実施例で詳しく説明する。ところで、例えば、平文ファイル１４１が選択された場合、まず、ユーザ・インターフェイス１１１１は、平文ファイル名をファイル暗号化手段１１６に渡す。ファイル暗号化手段１１６は、暗号化する平文ファイル名１４１を受け取ると、暗号ファイル名を作成する（ステップ６００３）。この暗号ファイル名は、暗号化したファイルに対してそれぞれユニークになるように、例えば、暗号化処理の回数のカウンタ値等から作成したシリアル番号と特定文字を組み合わせて生成する。次に、復号化の際に、元の平文ファイル名に戻すため、暗号ファイル名と１４１の平文ファイル名のセットを内部データ暗号鍵１２０と内部データ暗号・復号化手順１１８により暗号化した後、ファイル名変更情報１２１３１としてディスク４に格納する（ステップ６００４）。次に、ファイル暗号化手段１１６は、平文ファイル１４１のディスク４上での位置情報（平文ファイル１４１が格納されていたディレクトリの位置情報）を内部データ暗号鍵１２０と内部データ暗号・復号化手段１１８により暗号化した後、ファイル位置情報１２１４１としてディスク４に格納する（ステップ６００５）。次に、平文ファイル１４１のデータをディスク４より読みだし、内部データ暗号鍵１２０と内部データ暗号・復号化手順１１８により復号化したファイル暗号鍵１２１２を用いて、データ暗号・復号化手段１１９により暗号化し、暗号ファイル・データ１５１１として、ディスク４に格納する（ステップ６００６）。以上がファイルの暗号化処理である。複数の平文ファイルを対象として、ファイル暗号化処理を開始した場合には、ステップ６００３～ステップ６００５の処理を繰り返す（ステップ６００７）。ただし、以上の手順は一例であり、特に複数ファイルを暗号化する場合、手順を変えて、複数ファイルに対するファイル名変更情報やファイル位置情報等をまとめて暗号化して格納する等により、さらに、処理を高速化する等の工夫も本発明において可能なことは、言うまでもない。

【００５１】次に、図９のフローチャートにより、ファイル復号化時の処理手順について説明する。例えば、ファイル暗号化のメタファを指して、マウス押下を２回連続的に行う（以後、ダブルクリックと称す）等の操作を行い、ユーザ・インターフェイス１１１２に対して起動をかけると、ユーザ・インターフェイス１１１２は、ファイル復号化処理を開始する（ステップ７００１）。これらのユーザ・インターフェイスについては、後述の実施例で詳しく説明する。ユーザ・インターフェイス１１１２は、ファイル復号化の処理として、まず、ユーザの認証を行うために、ユーザにパスワードの入力を要求する（ステップ７００２）。ユーザがパスワード入力すると、ユーザ・インターフェイス１１１２は、そのパスワードをユーザ認証手段１１５に渡す。ユーザ認証手段１１５は、パスワードを受け取ると、暗号化されているパスワード１２１１をディスク４より取り出し、内部データ暗号鍵１２０と内部データ暗号・復号化手順１１８により復号化して、ユーザが入力したパスワードと比較し、正規ユーザかどうかを確認する（ステップ７００３、７００４）。不正パスワードで一致しない場合ユーザにメッセージを出す等して警告し処理を終了する（ステップ７００５）。一方、パスワードが一致した場合、は、ユーザ・インターフェイス１１１２は、ファイル復号化のためのウィンドウ表示処理を開始する。まず、暗号化されているファイルのリストをウィンドウ上に表示するため、ユーザ・インターフェイス１１１２は、ファイル復号化手段１１７に暗号化されたファイル名のリストを要求する。暗号化されたファイル名のリストに対する要求を受けると、ファイル復号化手段１１７は、ファイル名変更情報１２１３１、１２１３２と順次取り出し、それらを内部データ暗号鍵１２０と内部データ暗号・復号化手順１１８により復号化していく。そして、現在選択されている暗号化メタファに関連する暗号領域１２１上にある全てのファイル名変更情報を取得したところで、暗号化されているファイルの元の平文ファイル名のリストを作成し（ステップ７００６）、ユーザ・インターフェイス１１１２に返す。復号化を行った暗号領域１２１上にある全てのファイル名変更情報は、後で、ファイル復号化する際に使うため、適当なバッファに保持しておく。ユーザ・インターフェイス１１１２は、暗号化された平文ファイル名のリストを受け取ると、ウィンドウ上にそのリストを表示する（ステップ７００７）。次に、ウィンドウ上の暗号化された平文ファイル名のリストからユーザが復号化するファイルを選択すると（ステップ７００８）、ユーザ・インターフェイス１１１２

は、選択されたファイル名のリスト作成し、それをファイル復号化要求と共に、ファイル復号化手段１１７に渡す。ファイル復号化手段１１７は、ファイル復号化要求を受け取ると、まず、ファイル暗号鍵１２１２を読みだし、内部データ暗号鍵１２０と内部データ暗号・復号化手段１１８によりファイル暗号鍵１２１２を復号化しておく。その後、ファイル復号化要求と、一緒に受け取った、ユーザが選択したファイル名のリスト上のファイル名を順次取り出し、全暗号化ファイルのリスト作成時に復号化してバッファに保持しておいたファイル名変更情報の平文ファイル名から一致するファイル名を検索し、暗号ファイル・データ領域１５１に格納された暗号ファイル名に変換する（ステップ７００９）。そして、この暗号ファイルに対応したファイル位置情報を暗号データ領域１２１上のファイル位置情報から取得し元のファイルのディスク４上での位置を特定する（ステップ７０１０）。さらに、変換した暗号ファイル名の暗号ファイルのデータを暗号ファイル・データ１５１から読みだし、復号化しておいたファイル暗号鍵１２１２を用いて、データ暗号・復号化手段１１９により復号化し、ディスク４の元の位置に平文ファイルとして格納する（ステップ７０１１）。これらファイル復号化手段１１７のステップ７００９～ステップ７０１１の処理をユーザが選択したファイル全てに対して繰り返す（ステップ７０１２）。以上がファイルの復号化処理である。

【００５２】上記図７～９の各処理は、それぞれ個別に、または、一括して、計算機が読み取り可能なディスクや半導体メモリにプログラムの形で記述することができる。その様態も本発明に含まれる。

【００５３】次に、パーソナル・コンピュータ上で、Graphical User Interface（以下、GUIと称す）によるユーザ・インターフェイスを実現する米国マイクロソフト社のオペレーティング・システム"MS-Windows"（MS-Windowsは米国マイクロソフト社の登録商標）に本発明を適用した一実施例におけるユーザ・インターフェイスについて、画面の具体的イメージ示す図を用いて説明する。

【００５４】また、本実施例では、日常生活においてセキュリティ機能実現する道具としては最も一般的な金庫を模倣した"金庫フォルダ"をファイル暗号化メタファとして実現した。このような日常性のあるものをメタファに使うことにより、簡便操作と合わせてエンドユーザにも気軽に、高度なセキュリティ機能を操作できるようにした。

【００５５】図１０は、ファイル暗号化メタファの登録機能を実現する金庫ファルダ登録／削除ユーティリティのウィンドウのイメージを示したものである。ユーザが、新規登録ボタンをマウスで指して選択し、マウスのボタンを押下し、すぐ離す操作（以後、マウスで指して選択し、マウスのボタンを押下し、すぐ離す操作をクリックと称す）により、金庫フォルダの新規登録に起動をかけると、図１１に示す新規フォルダ登録ウィンドウを表示する。

【００５６】本実施例では、図６の実施例で説明したように、複数の暗号化メタファの登録を実現する。そのために、図１１の新規フォルダ登録ウィンドウでは、複数の金庫フォルダを登録した場合に、ユーザがそれぞれのフォルダの区別を付けるための、フォルダ名称の入力を行うようにした。また、図１１の新規フォルダ登録ウィンドウでは、ユーザの認証、および、暗号鍵を生成するためのベースとなるパスワード入力を行う。入力ミスを防止するためにパスワードの再入力要求も出す。

【００５７】図１２は、前記の新規フォルダ登録操作により、金庫フォルダのメタファとして金庫の形をしたアイコンが、MS-Windowsのプログラム実行ユーティリティであるプログラム・マネージャに登録された状態を示す。新規フォルダ登録操作を繰り返し、複数の金庫フォルダを登録すると、金庫フォルダー覧ウィンドウには、アイコン下部の名前の異なる複数の金庫フォルダ・アイコンが登録される。

【００５８】図１３は、図１０と同じ金庫ファルダ登録／削除ユーティリティのウィンドウで、既に、登録してある金庫フォルダを削除する操作を示したものである。図の様に登録してある金庫フォルダの名前を登録フォルダー覧を示す表示エリアで、マウスによりクリックして金庫フォルダを選択し、削除ボタンを選択すると、図１４のフォルダ削除ウィンドウが表示される。そこで、金庫フォルダ登録時に入力したパスワードを入力すると金庫フォルダは、削除される。この削除機能は、図６のブロック図で示した実施例では便宜上説明しなかったが、削除した金庫フォルダに対応した暗号データ領域のファイル、および、暗号ファイル領域のディレクトリとその下の暗号ファイルを削除することによりに実現できる。

【００５９】ところで、図１２の状態では、暗号化、および、復号化を行うプログラムをプログラム・マネージャに登録したものの、まだ、実行はされていない。しかし、一旦、プログラム・マネージャに金庫フォルダ・アイコンが登録されると、例えば、金庫フォルダー覧ウィンドウ上の金庫フォルダ・アイコンをマウスで２回連続にクリック操作（以後、マウスで２回連続にクリック操作することをダブル・クリックと称す）することで、金庫フォルダの暗号化、および、復号化を行うプログラムを実行することができる。図１５は、上記の操作で、金庫フォルダのプログラム実行した場合、金庫フォルダ・アイコンを示したものである。実行時の金庫フォルダのアイコンは、一般のプログラムの実行状態と同様に、MS-Windowsの背景となる壁紙領域に表示される。この状態で、金庫フォルダ・アイコンを操作することにより非常に簡便にファイル暗号化、復号化が可能となる。

【００６０】図１６は、実行状態の金庫フォルダ・アイコンより、複数のファイルの暗号化を行った画面を示し

たものである。まず、MS-Windowsのファイル管理ユーティリティであるファイル・マネージャのファイル名のリストを表示するウィンドウ上で、選択する複数のファイル名の上をマウスを押下しながら移動し、選択ができたところで離す（マウスのボタンを押下しながらマウス移動し、マウスを離す操作を以後ドラッグ・アンド・ドロップと称す）操作により、暗号化対象の複数のファイルを選択しておく。選択したファイル群で、再び、ドラッグ・アンド・ドロップ操作を開始し、金庫フォルダ上で、ドロップ（マウスのボタン離す操作）を行うだけで、選択した複数ファイルが暗号される。このように、金庫フォルダを使えば、実行してアイコン表示の状態にしておくだけで、ファイル・マネージャ等を介して、ドラッグ・アンド・ドロップという極めて簡便な操作でいつでもファイルを暗号化できる。また、図６のブロック図の実施例でも説明したように、金庫ファイルという暗号化メタファ登録時に、ユーザの認証に用いるパスワードから内部で自動的に暗号鍵を生成するため、ユーザが暗号鍵を意識しなくてすむことと、暗号化の際には、暗黙にその暗号鍵用いて暗号化するため、ユーザ認証を必要としないことが操作の簡便化に非常に効果的である。これにより、例えば、金庫フォルダをMS-Windows実行時に自動的に実行される様にしておけば、ユーザは、プライベートな情報のメモや業務に関連した機密文書を作成した場合にいつでも気軽にこれら情報ファイルを、暗号鍵を用いた高度な暗号化機能により暗号化し、第三者にのぞかれる心配なく保存できるので非常に便利である。

【００６１】もちろん、気軽に暗号化可能なために不用意に暗号化してしまう心配を持つユーザに対しての、例えば、金庫フォルダ実行後、最初の暗号化操作の場合のみパスワードによる認証を行う等の機能についても、図６のブロック図において、ファイル暗号化のユーザ・インターフェイス１１１に暗号化処理の回数をカウントするカウンタを設け、最初に暗号化処理に起動がかかった場合にのみユーザ認証手段１１５によってユーザ認証行うことで容易に実現可能であり、また、こうした、動作の選択を金庫フォルダの登録時の選択肢としてユーザに選択させることができる。

【００６２】次に、本実施例では、図１５の状態で、金庫フォルダをダブル・クリックすることによりファイルの復号化処理を起動するようにした。金庫フォルダをダブル・クリックすると図１７のパスワード入力ウィンドウを表示するユーザが、金庫フォルダ登録時に指定したパスワードと一致していれば図１８のファイル復号化ウィンドウがオープンできる。言うまでもなく、パスワードが間違っていれば、ファイル復号化ウィンドウをオープンできないので、パスワードを知らない第３者は、暗号化したファイルにアクセスすることはできない。

【００６３】図１８のようにファイル復号化ウィンドウでは、既に、暗号化して金庫フォルダに格納してあるファイルのリストを表示する。ファイルの復号化は、この暗号化したファイルのリスト上で、復号化したいファイル名をマウスでクリックして、図１９に示すように、選択した後、取り出しボタンをクリックし、ディスク上の暗号化前に格納されていたディレクトリに元の平文に戻して格納する。また、同じように、マウスによりファイルを選択して、図２０の様に削除ボタンをクリックすることで、ファイルの削除を行えるようにした。

【００６４】この復号化ウィンドウのリストで参照しないと、暗号化したファイルは、図６のブロック図の実施例でも説明したように平文の時のファイル名をシリアル番号等によるファイル名に変更しているために、ファイル・マネージャ等のファイル管理ユーティリティで、金庫フォルダの暗号ファイル領域１５１等を覗いても何のファイルかもわからないのでより機密性を保持している。

【００６５】

【発明の効果】本発明によれば、計算機の仕組みや操作に精通しないエンドユーザでも直感的で簡便な操作により、気軽にファイル等のデータの暗号化・復号化を活用することが可能であり、計算機上の個人情報や業務に関連した機密情報等のセキュリティの向上を容易に図ることが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施例を示すブロック図である。

【図２】本発明を適用する基本的なシステム構成示すブロック図である。

【図３】本発明の別の実施例を示すブロック図である。

【図４】本発明の別の実施例を示すブロック図である。

【図５】本発明の別の実施例を示すブロック図である。

【図６】本発明の別の実施例を示すブロック図である。

【図７】ファイル暗号化メタファ登録処理の手順を示すフロチャートである。

【図８】ファイル暗号化処理の手順を示すフロチャートである。

【図９】ファイル復号化処理の手順を示すフロチャートである。

【図１０】本発明の一実施例である金庫フォルダ登録／削除ユーティリティ・ウィンドウを示す図である。

【図１１】金庫フォルダの新規フォルダ登録ウィンドウを示す図である。

【図１２】金庫フォルダが登録されたプログラム・マネージャのウィンドウを示す図である。

【図１３】本発明の一実施例である金庫フォルダ登録／削除ユーティリティ・ウィンドウを示す図である。

【図１４】金庫フォルダのフォルダ削除ウィンドウを示す図である。

【図１５】金庫フォルダを実行した場合のアイコンを示す図である。

【図１６】ファイル・マネージャを介して、金庫フォル

21

ダでファイルの暗号化を行う操作画面を示す図である。

【図１７】金庫フォルダでウィンドウをオープンするためのパスワード入力ウィンドウを示す図である。

【図１８】金庫フォルダの復号化ウィンドウを示す図である。

【図１９】金庫フォルダの復号化ウィンドウでのファイルの復号化操作を示す図である。

【図２０】金庫フォルダの復号化ウィンドウでのファイルの削除操作を示す図である。

【符号の説明】

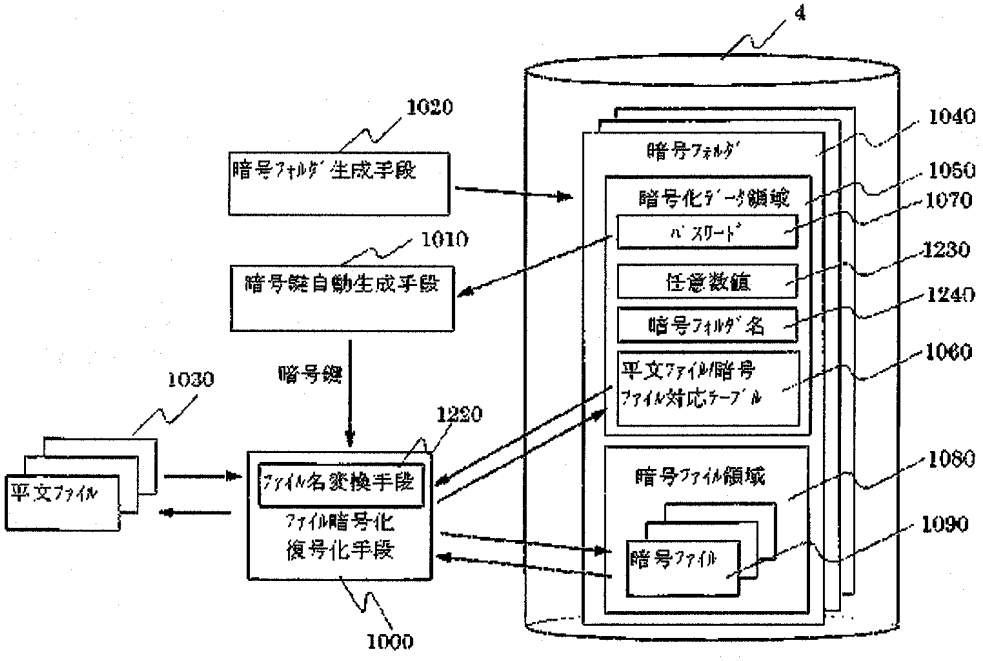
１･･･CPU、２･･･ROM、３･･･RAM、４･･･ディスク、５･･･ディスプレイ、６･･･キーボード、７･･･マウス、８･･･システム･バス、１１･･･ファイル暗号化制御、１１１･･･ユーザ･インターフェイス、１１２･･･ファイル暗号化領域生成手段、１１３･･･パスワード登録手段、１１４･･･暗号鍵生成登録手段、１１５･･･ユーザ認証手段、１１６･･･ファイル暗号化手段、１１７･･･ファイル復号化手段、１１８･･･内部データ暗号･復号化手段、１１９･･･データ暗号･復号化手段、１２･･･ファイル暗号化制御データ、１２１、１２２、１２３･･･暗号化データ領域

22

＊、１３･･･ファイル管理手段、１４１、１４２･･･平文ファイル、１５１、１５２、１５３･･･暗号ファイル領域、１０００･･･ファイル暗号化復号化手段、１０１０･･･暗号鍵自動生成手段、１０２０･･･暗号フォルダ生成手段、１０３０･･･平文ファイル、１０４０･･･暗号フォルダ、１０５０･･･暗号化データ領域、１０６０･･･平文ファイル／暗号ファイル対応テーブル、１０７０･･･パスワード、１０８０･･･暗号ファイル領域、１０９０･･･暗号ファイル、１１００･･･暗号フォルダ・ファイル生成手段、１１１０･･･暗号フォルダ生成手段、１１２０･･･暗号フォルダ・ファイル、１１３０･･･暗号ファイル領域データ、１１４０･･･自己復号化プログラム生成手段、１１５０･･･復号化プログラム、１１６０･･･自己復号化プログラム、１１７０･･･復号化手段、１１８０･･･認証手段、１１９０･･･カウンタ、１２００･･･暗号フォルダ無効化手段、１２１０･･･暗号フォルダバックアップ手段、１２３０･･･任意数値、１２４０･･･暗号フォルダ名、１２２０･･･ファイル名変換手段、１３００･･･FD、１４００･･･ネットワーク

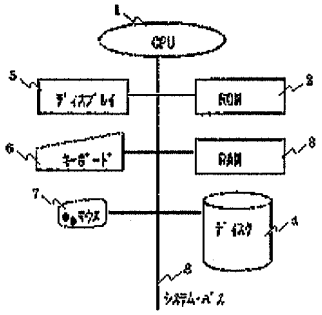
【図１】

図１



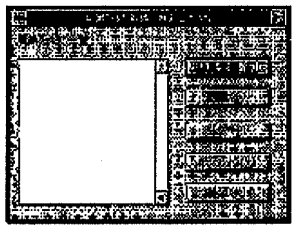
【図２】

図２



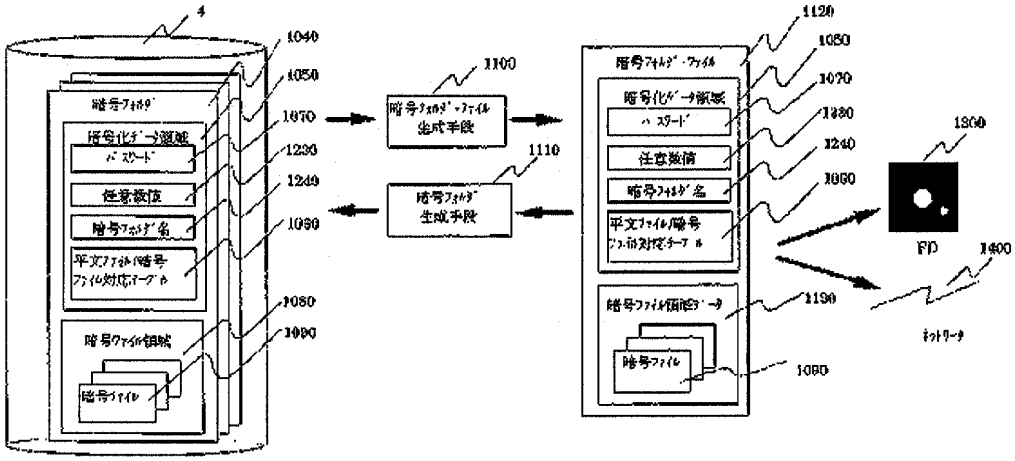
【図１０】

図１０



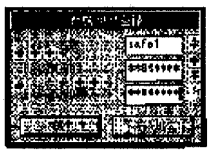
【図３】

図３



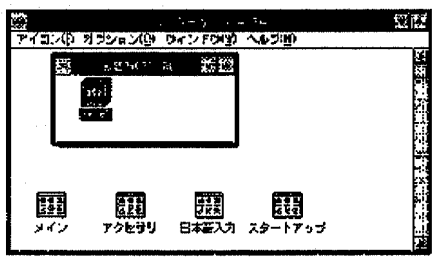
【図１１】

図１１



【図１２】

図１２



【図１５】

図１５

【図4】

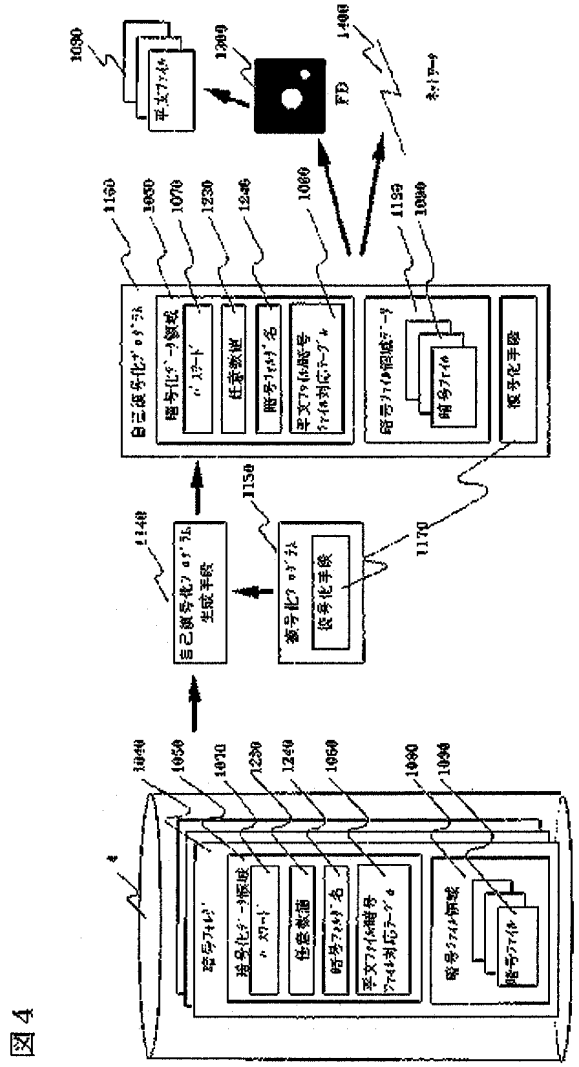


図4

【図5】

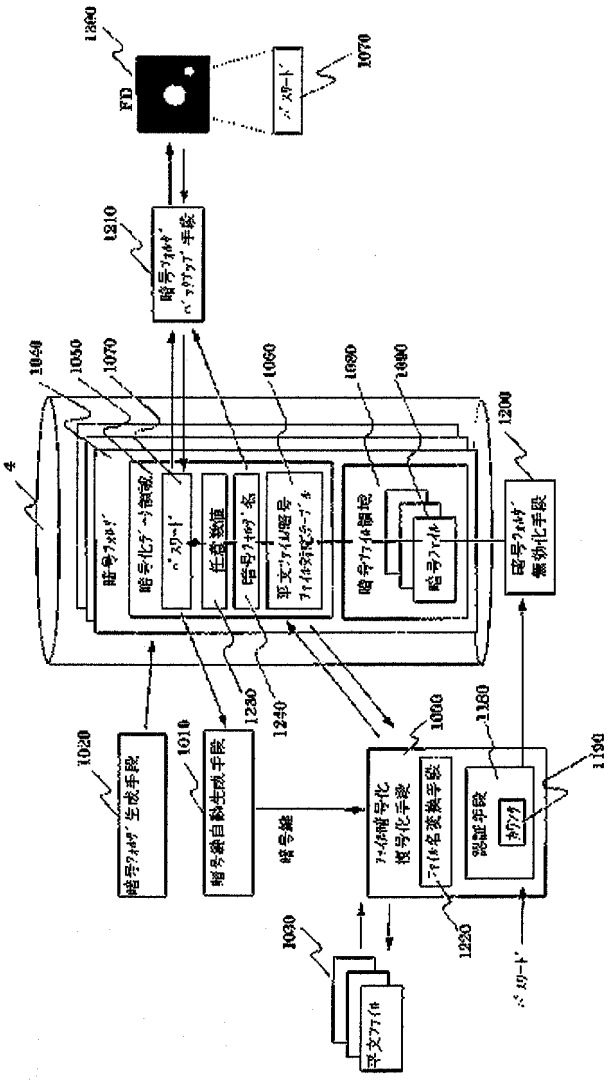

FD
暗号ファイル復号手段
暗号化データ抽出
パスワード
任意数値
暗号ファイル名
平文ファイル暗号化データ
暗号ファイル領域
暗号ファイル
暗号ファイル書込手段
暗号ファイル生成手段
暗号鍵自動生成手段
暗号鍵
ファイル暗号化復号手段
ファイル名変換手段
認証手段
判定
平文ファイル

図5

【図6】

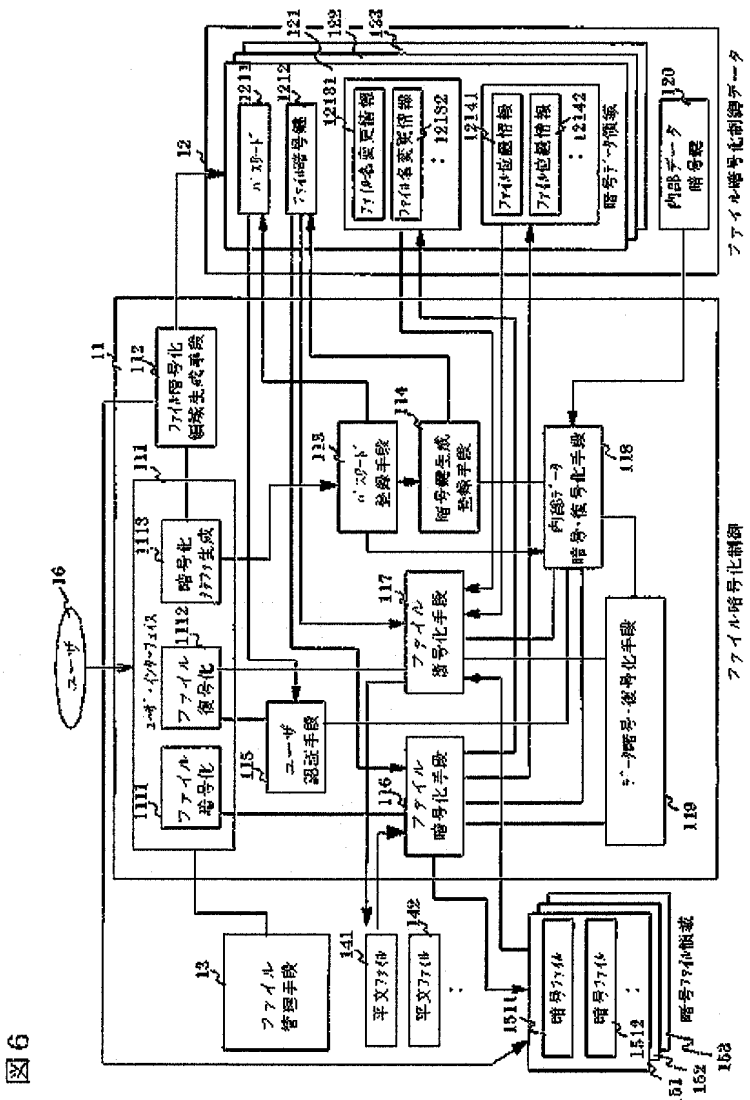
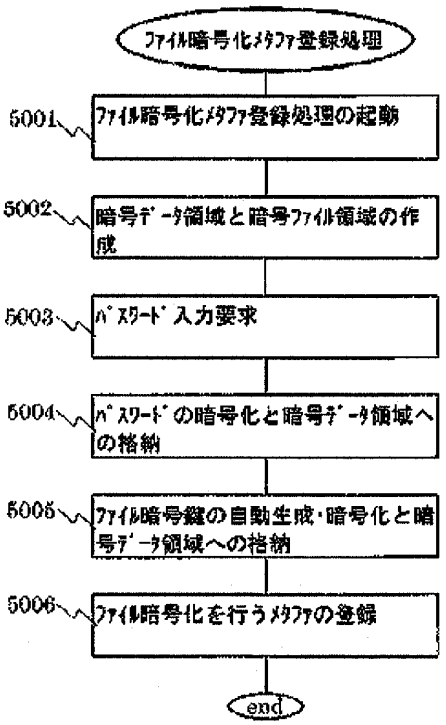

ユーザ
ユーザ・インタフェース
ファイル暗号化
ファイル復号化
暗号化ファイル生成
ファイル暗号化鍵生成手段
ユーザ認証手段
ファイル暗号化手段
ファイル復号化手段
ハンドシェイク処理手段
暗号鍵生成処理手段
内部データ暗号・復号化手段
ファイル暗号化制御
ファイル管理手段
平文ファイル
暗号ファイル
ハンドシェイク鍵
ファイル暗号化鍵
ファイル名変更情報
ファイル名変更情報：12152
ファイル位置情報
ファイル位置情報：12142
暗号データ領域
内部データ暗号鍵
ファイル暗号化制御データ

図6

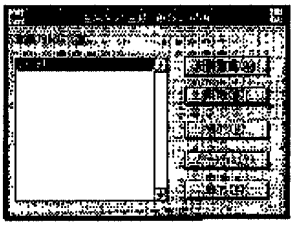
【図７】

図７



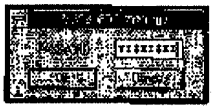
【図１３】

図１３



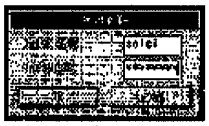
【図１７】

図１７



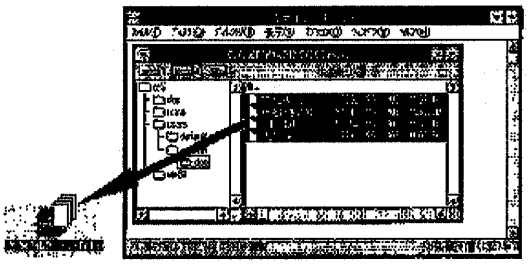
【図１４】

図１４



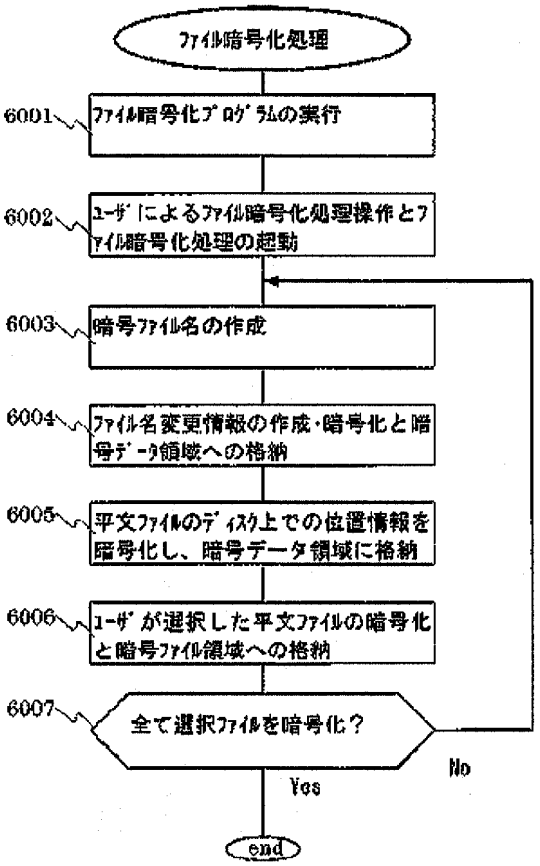
【図１６】

図１６



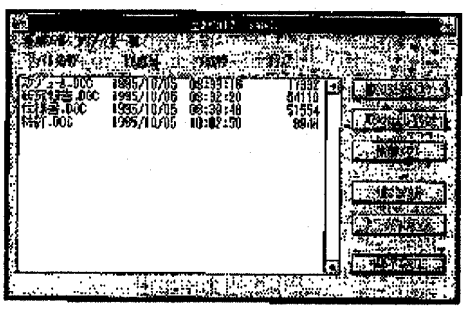
【図８】

図８



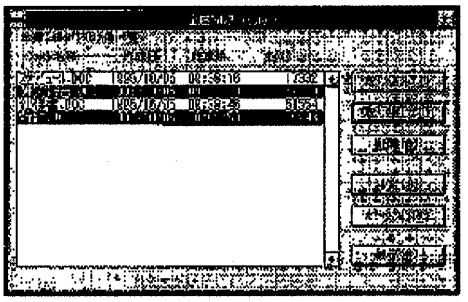
【図１８】

図１８



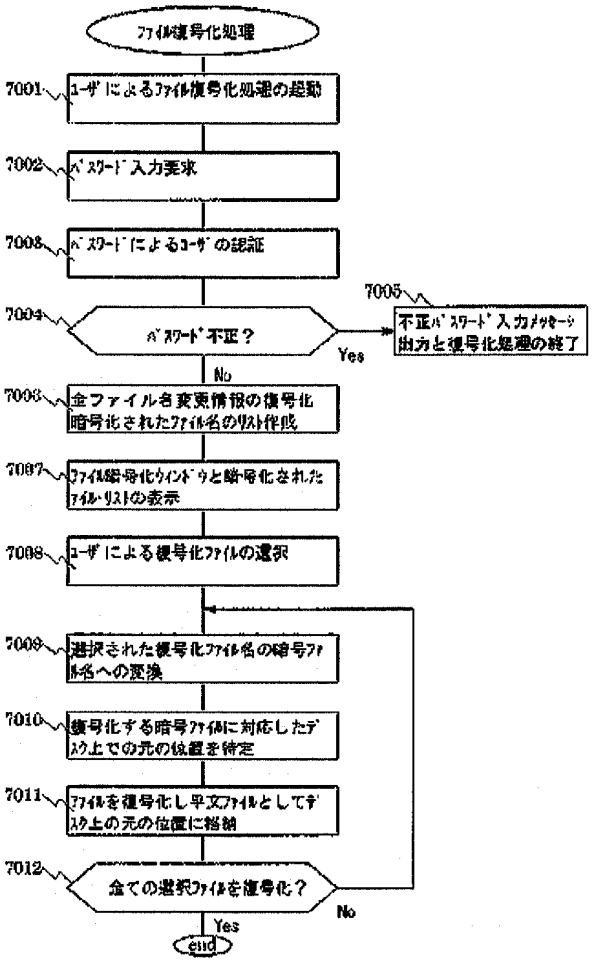
【図１９】

図１９



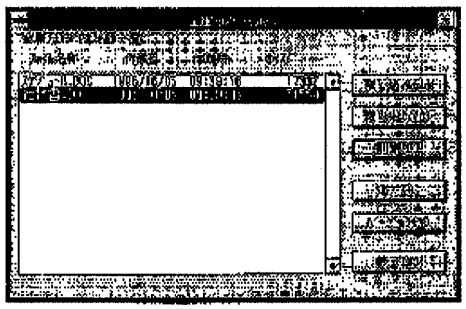
【図９】

図９


ファイル復号化処理
7001
ユーザによるファイル復号化処理の起動
7002
パスワード入力要求
7003
パスワードによるユーザの認証
7004
パスワード不正？
Yes
7005
不正パスワード入力メッセージ出力と復号化処理の終了
No
7006
全ファイル名変更情報の復号化暗号化されたファイル名のリスト作成
7007
ファイル復号化ウインドウと暗号化されたファイル・リストの表示
7008
ユーザによる復号化ファイルの選択
7009
選択された復号化ファイル名の暗号ファイル名への変換
7010
復号化する暗号ファイルに対応したディスク上での元の位置を特定
7011
ファイルを復号化し平文ファイルとしてディスク上の元の位置に格納
7012
全ての選択ファイルを復号化？
No
Yes
end

【図２０】

図２０



フロントページの続き

(51)Int.Cl.°		識別記号	庁内整理番号	FI		技術表示箇所
Ｇ０９Ｃ	1/00	６３０	7259－5J	Ｇ０９Ｃ	1/00	６３０Ｚ
		６６０	7259－5J			６６０Ｄ
Ｈ０４Ｌ	9/08			Ｈ０４Ｌ	9/00	６０１Ａ
	9/32					６０１Ｚ
						６７３Ａ

(72)発明者　古川　博
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　住友　正人
神奈川県海老名市下今泉810番地株式会社日立製作所オフィスシステム事業部内

(72)発明者　小林　祐一
神奈川県海老名市下今泉810番地株式会社日立製作所オフィスシステム事業部内